Certificaat of smartcard-gebaseerde verificatie configureren voor ISE-beheer

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram ISE samenvoegen in actieve map Map-groepen selecteren Wachtwoord voor actieve map inschakelen voor beheertoegang Geef externe identiteitsgroepen aan beheergroepen op Vertrouwd certificaat importeren Certificaatverificatieprofiel instellen Op client gebaseerde verificatie inschakelen Verifiëren Problemen oplossen

Inleiding

In dit document wordt beschreven hoe u clientadapterverificatie op basis van certificaten voor de toegang tot Identity Services Engine (ISE) kunt configureren. In dit voorbeeld, authenticeert de ISE-beheerder aan de hand van het gebruikerscertificaat om Admin-toegang te verkrijgen tot de Cisco Identity Services Engine (ISE) Management GUI.

Voorwaarden

Vereisten

Cisco adviseert om kennis van deze onderwerpen te hebben:

- ISE-configuratie voor wachtwoord- en certificeringsverificatie.
- Microsoft Active Directory (AD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine (ISE) versie 2.6
- Windows Active Directory (AD) Server 2008 release 2
- Certificaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als het netwerk live is, zorg er dan voor dat u de mogelijke impact van elke configuratie begrijpt.

Configureren

Gebruik dit gedeelte om het clientcertificaat of de slimme kaart te configureren als een externe identiteit voor beheertoegang tot de Cisco ISE-beheerGUI.

Netwerkdiagram



ISE samenvoegen in actieve map

- 1. Kies Administratie > Identity Management > Externe identiteitsbronnen > Actieve map
- 2. Maak een instantie van de Actieve Map met de **naam van het Punt samen** te voegen en **AD domein** in Cisco ISE.
- 3. Klik op Inzenden.



4. Sluit alle knooppunten aan op de juiste gebruikersnaam en wachtwoord in de melding.

dentity Services Engine Home →	Context Visibility + Ope	rations + Policy -Admir	nistration 🔹 Work Co	enters		License Warning 🔺	٩,	0 0	a -		
System Identity Management Network	System + Identify Management + Network Resources + Device Portal Management px:0+id Service + Freed Service + Threat Centric NAC										
+ Identities Groups External Identity Sources	Identities Groups External Identity Sources Identity Source Sequences Settings										
External Identity Sources	Connection	Whitelisted Domains Pass	siveID Groups	Attributes Advance	ed Settings						
	* Join Point Name * Active Directory Domain	AD mydomain.com		ı ı					Î		
DDAP ODBC RADIUS Token	양 Join 양 Leave 및 Tes	t User 🔮 Diagnostic Tool 😵 Re	efresh Table Status	Domain Controller	Site						
RSA SecuriD	ise2.mydomain.com	STANDALONE	🖾 Operational	WIN-58UQFTHFNIP.mydomai	Default-First-Site-Name						
Calification and the Providence Social Login		Join Domain Please specify the credentials (* AD User Name * Passw Specify Organizational Unit Store Credentials	required to Join ISE no e @ [e @ e @	de(;) to the Active Directory Domain	X Cancel						

5. Klik op Opslaan.

Map-groepen selecteren

- 1. Maak een externe Administrator-groep en stuur het naar de actieve directory groep.
- 2. Kies Administratie >identiteitsbeheer > Externe identiteitsbronnen > Actieve map > Groepen > Groepen uit Map selecteren.
- 3. Neem ten minste één AD-groep op waartoe de beheerder behoort.

es	Identity Source Sequences + Settings		
	Select Directory Groups		×
	This dialog is used to select groups from the Dire	ictory.	
	Domain mydomain.com	v	
	Name Filter *ISE-*	SID Filted *	
	Retrieve Groups 2 Groups Retrie	aved	
0	Name Name	Group SID Group Type	
	wydomain.com/ISE-Admin	S-1-5-21-4009324561-3650473562-621564990-1 GLOBAL	
	widomain.com/Users/ISE-RO	S-1-5-21-4009324561-3650473562-621564990-11 GLOBAL	
Ē			
		ОКСа	ncel

4. Klik op Opslaan.

Wachtwoord voor actieve map inschakelen voor beheertoegang

- 1. Actieve directory-instantie inschakelen als op een wachtwoord gebaseerde verificatiemethode die eerder tot ISE is toegetreden.
- 2. Kies **Beheer > Systeem > Admin toegang > Verificatie**, zoals in de afbeelding.

cisco Identity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System → Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Deployment Licensing + Certific	ates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings
O Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
Administrators	Password Based Algentity Source AD:AD
 Settings 	
	O Client Certificate Based
	Save Reset

3. Klik op **Opslaan**.

Opmerking: De op wachtwoord gebaseerde echtheidsconfiguratie is vereist om op certificaat gebaseerde verificatie mogelijk te maken. Deze configuratie moet worden omgekeerd na

een succesvolle configuratie van op certificaten gebaseerde verificatie.

Geef externe identiteitsgroepen aan beheergroepen op

In dit voorbeeld wordt de externe AD-groep toegewezen aan de standaard Admin-groep.

- 1. Kies Beheer > Systeem > Admin Toegang >Beheerders >Admin Groepen > Super Admin.
- 2. Controleer het type als extern en selecteer de AD groep onder Externe groepen.

dentity Services Engine	Home → Context Visibility → Operations → Policy ▼Administration → Work Centers	License W					
▼ System → Identity Management	t I Network Resources I Device Portal Management pxGrid Services I Feed Service I Threat Centric NAC						
Deployment Licensing + Certifi	ficates → Logging → Maintenance Upgrade → Backup & Restore ▼ Admin Access → Settings						
Authentication Authorization	Admin Groups > System Admin Admin Group * Name System Admin						
▼ Administrators	Description Access permission for Operations tab. Includes System and data access permission for Admin Groups.						
Admin Users	Type 🗹 External						
Admin Groups	External Identity Source						
 Settings 	Name : AD						
* I mydomain.com/ISE-Admin O + Member Users							
	Status Email Username First Name Last Name						
	No data available						

- 3. Klik op **Opslaan**.
- 4. Kies Beheer > Systeem > Admin Access > Administrators > Admin Groepen > Alleen lezen Admin.
- 5. Controleer het type als **extern** en selecteer de AD groep onder **Externe groepen**, zoals in de afbeelding weergegeven.

Cisco Identity Services Engine Home → Context Visibility → Operations → Policy ~ Administration → Work Centers Licen ~System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC Deployment Licensing → Certificates → Logging → Maintenance Upgrade → Backup & Restore ~ Admin Access → Settings
System + Identity Management + Network Resources + Device Portal Management pxGrid Service + Feed Service + Threat Centric NAC Deployment Licensing + Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings
Deployment Licensing + Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings
0
Authentication Admin Groups > Read Only Admin Admin Group
* Name Read Only Admin
* Administrators Description Access Permission for admin with read-only functionality
Admin Users Type 🗸 External
Admin Groups External Identity Source
Settings Name: AD
v External Groups @
* 📗 mydomain.com/Users/ISE-RO 🛛 📀 🕂
Member Users Users
👍 Add 👻 🗙 Delete
Status Email Username First Name Last Name
No data available
Save Reset

6. Klik op **Opslaan**.

Vertrouwd certificaat importeren

- 1. Importeer het certificaat van de certificaatautoriteit (CA) dat het certificaat van de klant bevestigt.
- 2. Kies beheerder > Systeem > Certificaten > Vertrouwd certificaat > Importeren.
- 3. Klik op Blader en kies het CA-certificaat.
- 4. Controleer het Vertrouwen op clientverificatie en het selectieteken Syslog, zoals in de afbeelding wordt weergegeven.

diate Identity Services Engine	Home → Context Visibility → Operations → Policy ▼Administration → Work Centers	License Warning 🔺	e,	0 0	•				
- System + Identify Management + Nebwok Resources + Device Portal Management pxOrid Services + Feed Service + Threat Centric NAC									
Deployment Licensing + Certifi	ates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings								
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests	Import a new Certificate into the Certificate Store * Certificate File Choose File DCcomDCmymainWpem Filendly Name Tusted For: Tusted For: Trust for authentication within ISE								
Certificate Penodic Check Setti Certificate Authority	Trust for client authentication and Syslog Trust for authentication of Cisco Services Validate Certificate Extensions								
	Description Cancel								

5. Klik op Inzenden.

Certificaatverificatieprofiel instellen

1. Kies Administratie >identiteitsbeheer > Externe identiteitsbronnen > Facebook-

verificatieprofiel > Toevoegen.

- 2. Naam profiel toevoegen.
- 3. Selecteer de gewenste eigenschap die de gebruikersnaam voor de beheerder in de certificaateigenschap bevat.
- 4. Als het AD-record voor de gebruiker het certificaat van de gebruiker bevat en het certificaat dat van de browser wordt ontvangen, wilt vergelijken met het certificaat in AD, voert u altijd binaire vergelijking uit en selecteert u de naam van de instantie die van de Active Directory is opgegeven.

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC	
Identities Groups External Identity Sources Identity Source Sequences Settings	
• Identitie @ roop Edenal Identity Source Identity Source > settings • Identitie @ roop = identity Source • Settingate Authentication Profiles Lid > New Certificate Authentication Profile • Construction Profile • Name • Clogin_Profile • Any Bools Status • Status • Status • Status • Status • Providers • Object • Auto-Auto-Object • Object • Status • Providers • Object • Object <td></td>	

5. Klik op Inzenden.

Opmerking: Hetzelfde certificatieprofiel kan ook worden gebruikt voor de op identiteit gebaseerde verificatie van het eindpunt.

Op client gebaseerde verificatie inschakelen

1. Kies Toediening > Systeem > Admin Access > Verificatie > Clientcertificaat voor verificatiemethode.

disco Identity Services Engine	Home + Context Visibility + Oper	rations + Policy - Administration + Work Centers
▼ System → Identity Management	Network Resources Device Portal I	Management pxGrid Services + Feed Service + Threat Centric NAC
Deployment Licensing + Certific	cates + Logging + Maintenance	Enabling Client Certificate-Based Authentication will cause an application server restart on all deployment
0		nodes. This will result in significant downtime for the system.
Authentication	Authentication Method	
Authorization	Authentication Type	Cancel
▼ Administrators	O Password Based	
Admin Users		* Identity Source (AD:AD *
Admin Groups	Client Cartificate Raced	
Settings	G Chent Centincate Dased	
	Save	

- 2. Klik op OK.
- 3. Kies het **profiel** van de **certificaatverificatie** dat eerder is ingesteld.
- 4. Selecteer de naam van de instantie Active Directory.

cisco Identity Services Engine	Home + Context Visibility + Operations + Policy Administration + Work Centers
▼ System	+ Network Resources + Device Portal Management pxGrid Services + Feed Service + Threat Centric NAC
Deployment Licensing → Certifi	icates → Logging → Maintenance Upgrade → Backup & Restore ▼Admin Access → Settings
G Authentication	Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings
Authorization	Authentication Type
▼ Administrators	O Password Based
Admin Users	
Settings	Client Certificate Based * Certificate Authentication Profile CAC_Login_Profile *
	* Identity Source AD:AD
	Save Reset

- 5. Klik op **Opslaan**.
- 6. ISE-services op alle knooppunten in de implementatieherstart.

cisco Identity Services Engine	Home → Context Visibility → Ope	erations + Policy -Administration		
▼ System → Identity Managemen	t + Network Resources + Device Portal	Management pxGrid Services + Feed	Service I Threat Centric NAC	
Deployment Licensing + Certif	ficates → Logging → Maintenance	The system will now restart.		
ġ				
Authentication	Authentication Method			
Authorization	Authentication Type			ок
✓ Administrators	Password Based			
Admin Users				
Admin Groups	Olivet Cutificate David			
▶ Settings	Client Certificate Based	* Certificat	e Authentication Profile CAC_Login_Profile	ž
			* Identity Source AD:AD	ž
	Save Reset			

Verifiëren

Controleer de toegang tot de ISE GUI nadat de servicestatus van de **Application Server** verandert in **gebruik.**

Super Admin Gebruiker: Controleer dat de gebruiker wordt gevraagd een certificaat te kiezen om in te loggen op de ISE GUI en krijgt Super Admin-rechten als het certificaat van een gebruikersdeel van de Super Admin Externe Identity Group is.





Alleen-lezen beheerder: controleer of de gebruiker een certificaat heeft gevraagd om in te loggen

op de ISE GUI en alleen Lezen-only Admin rechten heeft als het certificaat deel uitmaakt van een gebruikersgroep van de alleen-lezen Admin Externe Identity.

🕞 🔿 🧭 https://ise2.mydomain.com/



(⇐) (⇐) https://ise2.mydomain.com/admin/ (⇐) (⇐) Identity Services Engine ×								☆ 🖒	£33			
cisco Identit	/ Services Engine	Home	▶ Context Visibility	 Operations 	Policy	Administration	 Work Centers 	Read-Only	License Warning 🔺	Q,	e 0	~
Sum	Endpoints	Guests	Vulnerability	Threat	+						φ.	· .
METRI	CS Total Endp	oints 🚯		Active Endpoir	nts 🖸	R	jected Endpoints 🕄	Anoma	alous Behavior 🕲		- Ø	
<			0	¢ (0	Þ,	•	0		0	>	
# AUTHENTICATIONS Image: Construction of the second se						Ø	σx					
No data available.				No data available.			No o	data available.				
												l
∦ BYC	D ENDPOINTS	0	во×	ii Alar	MS 🛛		eσx	# SYSTEM SUMM	IARY 🛛	ø	σx	
Туре	rofile			Severity	Name	Oc	cu Last Occi	1 node(s)		All -	24HR -	
	No data a	vailable.		×				🔽 📄 ise2				~

Opmerking: Als Common Access Card (CAC) in gebruik is, geeft Smartcard het gebruikerscertificaat aan ISE nadat de gebruiker hun geldige superpin heeft ingevoerd.

Problemen oplossen

1. Gebruik de app start veilige opdracht om Cisco ISE te starten in een veilige modus die

tijdelijk toegangscontrole naar het Admin-portal **toestaat** en de configuratie en het opnieuw opstarten van de services van ISE **toestaat** met de **optie** van de opdrachttoepassing **stop** gevolgd door **ingang van de toepassing**.

2. De veilige optie biedt een manier van herstel als een beheerder onopzettelijk de toegang tot het Cisco ISE Admin-portal voor alle gebruikers sluit. Deze gebeurtenis kan voorkomen als de beheerder een onjuiste IP-toegangslijst instelt in het Beheer > Toegang > Instellingen > Access-pagina. De veilige optie omzeilt op certificaat gebaseerde verificatie en keert terug naar de standaard gebruikersnaam en wachtwoordverificatie voor loggen naar het Cisco ISE Admin-portaal.